STRATEGY RESEARCH PROJECT

ARMY TRANSFORMATION AND INFORMATION OPERATIONS: THE INTERNATIONAL LEGAL IMPLICATIONS

BY

LIEUTENANT COLONEL EARL E. MILLER
United States Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

ARMY TRANSFORMATION AND INFORMATION OPERATIONS: THE INTERNATIONAL LEGAL IMPLICATIONS

by

Lieutenant Colonel Earl E. Miller
United States Army

Colonel Ralph Ghent
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Earl E. Miller

TITLE: Army Transformation and Information Operations: The International Legal Implications

FORMAT: Strategy Research Project

DATE: 9 April 2002 PAGES: 34 CLASSIFICATION: Unclassified

As many nations throughout the world have become entrenched in what has been described as the information revolution, many legal parameters of information operations remain uncertain. Information is fast becoming a strategic resource that permeates every facet of the U.S. National Military Strategy. The proliferation of information-based technologies will substantially transform the Army's doctrine as well as its structure. The evolution of the information environment has specific legal implications within the international community. This paper examines these challenges and proposes to establish a framework for the inevitable global debate over related legal issues.

TABLE OF CONTENTS

PREFACE

I would like to first thank my project advisor, Colonel Ralph Ghent, for his advice, patience, and guidance in assisting me to complete this project. I would also be remiss if I didn't thank my wife Carolyn and my two boys, Mathew and Daniel, who sacrificed some of the "Best Year" of our life together for me to complete this project. The long hours spent on this project caused me to sometimes neglect those that I love and care for the most. Your understanding, support, and patience speak volumes about your love for me.

LIST OF ILLUSTRATIONS

ARMY TRANSFORMATION AND INFORMATION OPERATIONS: THE INTERNATIONAL LEGAL IMPLICATIONS

There are many aspects of information operations that are, as yet, shrouded in uncertainty.[1] As nations throughout the world become engaged in what many have described as the information revolution, several legal parameters of information operations remain ambiguous.[2] Information technology is fast becoming a strategic resource that permeates every facet of the U.S. National Security Strategy.[3] The proliferation of information-based technologies will substantially transform the Army's doctrine as well as its structure. The increasing complexity of the information environment has specific legal implications throughout the international community.

This paper discusses the importance of an integrated information operations strategy as an essential component of the Army's new transformation plan. It will identify challenges regarding information operations under international law, indicating how such laws may impact on information operations. The study concludes with recommendations for clarifying legal ambiguities surrounding information operations.

THE ARMY'S TRANSFORMATION VISION

The future ain't what it used to be!

—Yogi Berra

For the past fifty years, the U.S. Army has been structured to fulfill America's security requirements for the Cold War. Recently, our external strategic environment and security concerns have changed dramatically, necessitating restructuring. After the Soviet Union's demise and the Allied victory in the Gulf War, the Army was left without a clear strategic vision, a relevant force structure, or an evident threat upon which to base the Army's future force structure. This period of diminished threat, rather than events, has provided an opportunity for the Army transformation process.[4]

Responding to skeptics that the Army had failed to adjust to the new post-Cold War realities, Secretary of the Army Louis Caldera and Chief of Staff of the Army General Eric K. Shinseki unveiled their strategic vision on 12 October 1999 at the annual Association of the United States Army annual convention. The new vision was entitled "Soldiers on Point for the Nation - Persuasive in Peace, Invincible in War." The Army vision focuses on three areas: caring for people, maintaining the readiness to respond strategically throughout the world, and transforming the Army to dominate the entire spectrum of operations. This vision recognizes

that the Army's soldiers and their families are the centerpiece of Army capabilities and represent the most vital component of transformation. As General Shinseki stated, the purpose of this vision is to set the azimuth for the Army to meet the requirements of the 21st Century.[5]

Army transformation is a comprehensive undertaking that will incorporate the decisive warfighting capabilities of our heavy divisions and the strategic responsiveness inherent in our light divisions. To implement this vision, the Army established its comprehensive transformation strategy. The strategic vision will be enacted over several years. It must balance the challenges associated with transforming the operational force while simultaneously maintaining a trained and ready force able to respond to on-going crises and to deter war. The transformed fighting force will be more responsive, deployable, agile, versatile, lethal, survivable, and sustainable. To make this force more deployable, the Army must reduce the organization's overall footprint. To achieve the Army's vision, three separate forces were developed: the Legacy Force, the Interim Force, and the Object Force (see Figure 1).[6]

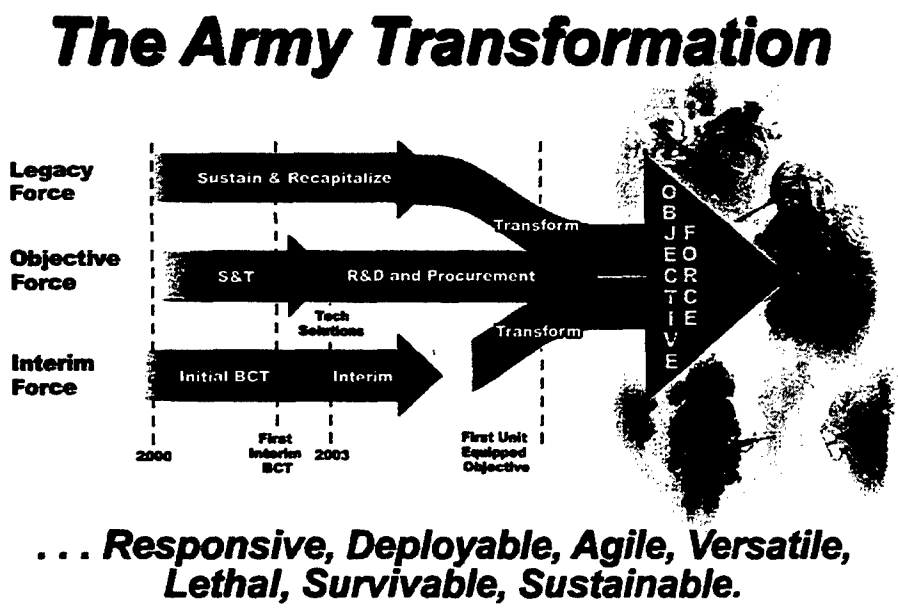

FIGURE 1

The first axis, the Legacy Force, re-capitalizes selected units and equipment from today's force structure, the primary ground combat maneuver platforms. Re-capitalization of legacy systems will not only increase the equipments' service life and reduce maintenance costs but will also improve logistical support requirements in the future. Over time, enhancements to Legacy Force equipment and systems will significantly improve the lethality and survivability of

these units. The Legacy Force will continue to be the Army's principal warfighting force for the near term.[7]

The second axis, the Interim Force, is a transitional force composed of the developmental Interim Brigade Combat Teams (IBCT). The Interim Force will develop the capabilities of the Objective Force within the constraints of emerging technologies. It will be light enough to display a smaller deployment signature on the battlefield, but heavy enough to be lethal against its adversaries. These combat teams will have the capability to deploy anywhere in the world in 96 hours. Every piece of equipment belonging to the force structure must be transportable by C-130 aircraft; this equipment will receive little, if any, support upon arriving at their area of operations for three days.[8]

The third axis proposes development of an Objective Force, which is the long-term goal of the Army's Transformation process. The Objective Force will be designed with the capabilities necessary to meet the challenges expected by the Army in 2020. The Objective Force realizes the Army's vision; it is the instrument through which the Army will retain its undeniable land force dominance over the full spectrum of operations. Currently, the Objective Force resides in the science and technology phase. Many challenges must be met to field a fully capable Objective Force. The current program goal is to have Objective Force technology produced by FY2008 and fielded by FY2010.[9]

General Shinseki's Army transformation strategy undoubtedly represents one of the military's most comprehensive institutional changes ever envisioned. This transformation mandates the Army to be strategically responsive and dominant across the entire spectrum of operations. Shinseki envisions a comprehensive program to increase the Army's capabilities. The vision encompasses force structure, equipment, vehicles, uniforms, as well as transformation of the way the Army thinks, trains, and fights. For the Army to maximize its full transformation potential, it must achieve information superiority. To achieve information superiority, the Army must develop an integrated information operations strategy.[10]

INFORMATION OPERATIONS: CAPTURING THE CONCEPT

> Dominating the information spectrum is as critical to conflict now as occupying the land or controlling the air has been in the past.
>
> —General Ronald R. Fogleman, Chief of Staff of the Air Force

Just what are Information Operations? Draft Army Field Manual 3-13 (Information Operations) defines information operations as "those actions taken to affect an adversary, and influence other's decision-making processes, information and information systems while

defending one's own information and information system." Accordingly, Joint Publications 3-13 (Joint Doctrine on Information Operations) articulates information operations as "those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. Information operations apply across all phases of an operation, throughout the range of military operations, and at every level of war." In short, information operations provide an integrated approach to managing and manipulating information and information networks.

The Army's doctrine of information operations consists of the following operational capabilities: psychological operations, electronic warfare, military deception, operational security, physical destruction, special information operations, computer network attack, counter deception, counter intelligence, counter propaganda, information assurance, civil affairs, public affairs, and physical security. These separate and distinct capabilities all fall under the umbrella of information operations: offensive and defensive. Offensive information operations entail the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence activities, to affect an adversary's decision-makers and promote specific objectives. Information operations may involve complex legal issues requiring careful national level coordination and approval. Defensive information operations integrate and coordinate policies, procedures, operations, and technology to protect and defend U.S. information and information systems. Four interrelated processes comprise defensive information operations: information environment protection, attack detection, capabilities restoration, and attack response.[11]

The ultimate goal of information operations is to attain and sustain information superiority across the entire spectrum of the battlefield. Accordingly, Joint Publication 3-13 defines information superiority "as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying the adversary's ability to do the same."

THE IMPORTANCE OF INFORMATION OPERATIONS

> Information, information processing and communications networks are at the core of every military operation. Throughout history, military leaders have regarded information superiority as a key enabler of victory.
>
> —Joint Vision 2020

Throughout the past century, we have used computers for storing information, analyzing data, and identifying trends. Now they have become an essential part of our daily lives, improving our efficiency and productivity while diminishing the manpower required to produce

the same output. We are increasingly managing our infrastructure – such as our transportation networks, power grids, and telecommunications– with computers rather than human control.

Advancement of information operations has become crucial to the Army as it attempts to gain a decisive advantage from the information-based technological revolution. The Army has dedicated enormous resources to develop information operations and its doctrinal applications throughout its transformation strategy. Further, an integrated information operations strategy that achieves information superiority is an essential element of the Army's vision for the 21st Century.

Following the Gulf War, military strategists throughout the world acknowledged new trends in warfare. They realized that military operations consisted of more than tanks, infantrymen, or artillery. They witnessed the Army integrating technological advancements in information operations throughout the conduct of war. The significance of timely and accurate information is absolutely essential to commanders, particularly as large force structures give way to smaller, highly trained, and more technically equipped forces. The J6 of the Joint Chiefs of Staff has asserted that, "Information systems are so important, they have become lucrative targets for numerous threats that we must deter and defeat. We conduct information operations to affect an adversary's information and information systems while defending our own information and information systems vital to achieving information superiority."[12]

NATIONAL POLICY & COMMAND AND CONTROL

> The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational, and the tactical situations, which advanced US technologies provide our forces.
>
> —Joint Pub 3-13

The current National Security Policy directing the military's implementation of information operations is set forth in Department of Defense Directive S-3600.1, Information Operations. This document provides general guidance and defines the roles and responsibilities of key personnel throughout the Department of Defense. Issued by the Chairman, Joint Chiefs of Staff, Joint Vision 2020 provides additional national security policy for the joint community regarding information operations.

The Secretary of Defense is responsible for the synchronization and coordination of information operations throughout the Department of Defense. The Chairmen of the Joint Chiefs of Staff serves as the Secretary's primary advisor on all matters relating to information

operations. Within the Joint Staff, the J3 Operations assigns the scope of responsibility for information operation.[13]

At the Joint Task Force level, an information operations officer is the focal point for all information operations functional areas. This individual coordinates all necessary actions through an information operations cell. The cell's primary mission is to coordinate and synchronize the detailed support necessary to plan and coordinate information operations. This cell consists of representatives from the J2 through J7 staff, the Staff Judge Advocate, Civil Affairs, targeting personnel, Public Affairs, imagery specialists, and various human intelligence representatives. Elements from other supporting organizations, such as the Joint Special Operations Task Force, may also be present.[14]

As information operations become more prominent throughout the Army's transformation strategy and doctrinal reorganization, specific modifications to the Army's force structure and doctrine will be increasingly necessary.

CHANGES TO THE ARMY'S FORCE STRUCTURE

> Iraq lost the war before it even began. This was a war of intelligence, electronic warfare, command and control, and counter intelligence. The Iraqi forces were blinded and deafened.
>
> —Soviet General S. Bogdanov,
> Chief of the General Staff, Center for Operational and Strategic Studies

Information operations are not new to the Army, but the Army is new to the information operations concept. As the Army reaps the benefits of the information revolution, it must be prepared to defeat adversaries with every tool technologically available. Additionally, it must be able to defend its own information systems, networks, and processes from disruption or destruction. Information operations provide the synergy to achieve full spectrum dominance.[15]

The information operations capabilities such as Psychological Operations, Operational Security, Counter Intelligence, Public Affairs and Electronic Warfare are not new to the Army's military strategy. Unfortunately, the synergistic effects inherent in these activities have not been utilized as a true force multiplier. In an attempt to obtain this synergy and achieve full spectrum dominance under the Army's transformation strategy, corps and division information operations will be synchronized by a new staff position called the Assistant Chief of Staff G7 (ACofS, G7) Information Operation Coordinator (IOCOORD). The G7 position will be coded and filled with Functional Area 30 (FA30) Information Operations Colonels. The Army's senior leaders established the G7 position as a coordinating staff officer. As such, the G7 will report directly to

the Chief of Staff, not the G3. The G7 will provide corps and division commanders the capability to plan, synchronize, and coordinate information operations assets necessary to attain information superiority. The IOCOORD must integrate all the different activities of IO to gain information and knowledge and improve friendly execution of operations, while denying an adversary similar capabilities and related activities. In short, the IOCOORD must be a strategic thinker and a staff officer – one who can analyze the information and derive the situation.[16]

Information operations are envisioned as a force multiplier for the Army's transformation. The Army must attain information superiority across the entire spectrum of operations. The creation of an ACofS G7 position and information operation staff section represent a significant milestone and will play an invaluable role towards attaining information superiority during an armed conflict. As commanders develop an integrated information operations strategy, the IOCOORD and his information operations cell will be challenged by international law.

THE INTERNATIONAL LEGAL IMPLICATIONS OF INFORMATION OPERATIONS

Our current National Military Strategy's use of information operations is constrained by a myriad of international legal challenges. Throughout the conduct of information operations, our strategic leaders must attend to several major bodies of international law that may impact on our information operations: the United Nations Charter, the Law of Armed Conflict, the International Telecommunications Law, Space Law, and related laws that address National Sovereignty and Foreign Domestic Laws. As information operations have become more relevant to the conduct of warfare, the legal community has begun raising questions regarding the interrelationship between international law and the conduct of information operations.

ANALYSIS - THE LEGAL IMPLICATIONS

> Exploiting information systems will readily cross international borders, we must be cognizant of what the law allows and will not allow. We must have good legal advice as we get into this.
>
> —General Ronald R. Fogelman, Chief of Staff, US Air Force

The proliferation of information technology and the increased interoperability of computers have greatly improved the utility of all kinds of information systems. Moreover, global communications are almost seamlessly interconnected and virtually instantaneous. The current technology revolution and more specifically the employment of information operations on the battlefield pose a significant challenge to the international legal system because innovations in technology may impinge on areas of international law that have not yet been applied to this emerging technology. We can anticipate contradictions among current legal principles. The

development of computers and telecommunications networks have created new possibilities for adversarial countries to attack one another, inflicting new forms of damage. Adversarial countries may use international networks to destroy an enemy's systems without ever physically stepping foot into the enemy's country. Additionally, the dual-use nature of many telecommunication networks and associated infrastructure is blurring the distinction between military and civilian targets.[17]

Information operations thus challenge international law in several ways: First, communication signals from one country can easily transit international borders and thus affect other telecommunication systems in distant countries. Such an intrusion could be regarded as a violation of territorial sovereignty, a universally accepted international legal principle. Next, the indefinable damage that an information operations attack may cause is essentially different than the physical damage caused by a traditional attack. The devastation caused by conventional weapons is easier to comprehend in the context of accepted views of war. In contrast, the destruction of an information network, power grid, or manipulation of data could produce intangible damage to a civilian or government agency. Finally, who is to say that an information operations attack is "an act of war?" It could be difficult to define their targets as legitimate military targets, or prohibited civilian targets. The injuries sustained by this type of situation could be a violation of the humanitarian law of war designed to protect noncombatants.[18]

THE SIGNIFICANCE OF CATEGORIZATION

The subject of how to categorize an information operations attack is extremely important. Whether or not an information operations attack can be considered an "act of war," or "aggression" is applicable to whether a forceful response can be justified as self-defense, or whether a retaliatory response would be proportionate to the original attack. [19]

Under international humanitarian law, characterization of attacks and the damage they cause is pertinent, specifically in those provisions that protect noncombatants from the consequences of an attack. First, if an information operations attack is not considered to be an act of "war," then humanitarian law will not be applicable. If humanitarian law does not apply, then countries may legally initiate information attacks without legal responsibility for the harm that civilians might suffer. Many information operations attacks that may not constitute "aggression" could certainly be perceived as a threat to the peace of another nation. After all, anything that would infuriate a government to the point that it might resort to military action could thus "threaten" the peace, even if the provocative action was not technically illegal. [20]

The complexity of characterizing certain types of information operations attacks as "war" or "aggression" under international law does not suggest that international legal institutions cannot respond to such attacks. Through its charter and Security Council, the United Nations has the authority to determine the existence of any "threat to the peace" or "act of aggression:" following such a determination, the Council would then recommend an appropriate response.[21] For example, if an information attack would intentionally cause the disruption of a nation's air traffic control system and thereby causes several planes to crash, the international legal community could consider the disruption an armed attack, which would then invoke the victim state's right to use in self-defense. [22]

UNITED NATIONS CHARTER

The primary source of current international law is the United Nations (UN). Specifically, within the UN Charter, three legal principles could challenge information operations. The first is Article 39; this article gives the UN Security Council the authority and responsibility to determine the existence of any "threat to the peace" or "acts of aggression" among nations. Another is Article 2, Section 4, which stipulates, "Members will refrain from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purpose of the UN." Finally, Article 51 recognizes the distinction between unlawful, aggressive use of force and a nation state's lawful right to defensive use of force: "Nothing in the present charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations until the Security Council has taken measures necessary to maintain peace and security." These three overarching international laws don't specifically discuss information attacks. But collectively they establish the scope and content of the Charter's prohibition on aggressive use of force, the responsibility of the Security Council to enforce this prohibition, and the right of all states to use force in self-defense. [23]

Consider one of the frequently asked questions regarding information operations: "Is a computer network attack an act of war?" Information attacks are not specifically addressed in the UN Charter, nor are they addressed in the modern international legal system. Consider a related question: Is an information attack an armed attack that justifies the use of force in self-defense? The UN Charter has not established that information attacks, particularly when they are not directly lethal or physically destructive, constitute the use of "force" or "armed attack." Although a consensus on the meaning of armed attack is of significant importance for effective application of the rules of international law on war, the phrase "information attack" is not defined

in the UN Charter. In both the above-mentioned situations, it seems likely that the international community would analyze the consequences of the computer network attack, rather than the mechanism itself. If the computer attack shuts down a nation's electric power grid causing extensive death and destruction, it may well be that no one would challenge the victim nation's claim that it was a casualty of an armed attack. Unfortunately, without UN clarification, there is no way to be certain how these principles of international law will be applied by the international community in the case of a computer network attack. [24]

The UN Charter simply neglects information operations. Its applicability to such operations will thus be subject to various interpretations. The international legal complexities pertaining to information operations make the UN charter an ideal starting point for determining the legal implications of information operations. [25]

THE LAW OF ARMED CONFLICT

The law of armed conflict (LOAC) is also commonly referred to as the law of war. This area of international law has significant bearing on information operations. It generally applies when there is a state of international armed conflict between two nations. It pertains to all parties to the conflict in exactly the same manner, no matter who may have started the conflict. This collection of laws has been derived from numerous international treaties as well as traditional international law. The two general principles of war that could affect information operations are military proportionality and necessity. Customary international law requires that all uses of force be proportional and necessary. These principles serve to limit and "civilize" military actions. [26]

The first principle, military proportionality, limits the amount of force that can be used against a military target to that which does not cause unnecessary collateral damage to civilian property or unnecessary suffering of civilians. Any information operations attack that would not have a reasonably predictable scope of destructive application would be prohibited by the first principle. A good example of this could be a logic bomb planted into a computer's circuitry and directed at a Department of Defense office, then activated at some later time. This type of information attack would be permissible. Conversely, an information attack that disrupts civilian telecommunications network could have devastating second and third order consequences in financial security, commerce and even various life-sustaining health care processes. This type of information attack would not be permissible under the proportionality principle. Warfare could, however, advance to a point where non-lethal, precision information strikes may be required by the customs of warfare over less precise, more destructive conventional methods. [27]

The second principle, necessity, concerns the cumulative impact of attacks against particular targets, which brings into question their characterization as military targets. Consider an information attack against systems that have a dual-use capability among a state's military forces and its civilian population. One way to resolve this challenge is to determine whether the target significantly contributes to the opponent's war-fighting capability such that its destruction would constitute a definite military advantage. If so, it may then be targeted. The principle of military necessity poses little problem to information operation strategies as long as the systems under attack are purely military targets. [28] For example, Desert Storm revealed that conventional military targets like electrical power grids and other telecommunications networks may perhaps be evolving into impermissible targets because of their interconnection and interdependence with systems serving the civilian populace. [29]

The LOAC principles seem to present no significant show stoppers to our information operation strategists. However, at the very least, the principles of LOAC should guide information attacks against specific targets. History has shown that the U.S. will be judged by the results of our actions, not by the particular weapons used. We must anticipate that information operations weapons will be judged by the same criteria as any other weapon.[30]

INTERNATIONAL TELECOMMUNICATIONS LAW

The United States has not entered into bilateral and multilateral communications treaties because international telecommunication laws provide the necessary foundation for handling most international communications challenges. For example, the International Telecommunications Charter (ITC) of 1982 and its fundamental organization, the International Telecommunications Union (ITU), apply directly to military information operations. The ITU formulates international telegraph and telephone regulations. It focuses primarily on interoperability and interference of the electromagnetic spectrum.[30]

Perhaps the most noteworthy application of this charter is Article 35, which stipulates that all stations, whatever their purpose, must be established and operated in such a manner as not to interfere with the radio services or communications of other member states. It defines "harmful interference" as anything that endangers the functioning of a radio navigation service or seriously degrades or obstructs a radio communications service. Some would agree that this article prohibits the use of a satellite station to jam or interrupt the communications of another state's radio service.[31]

However, Article 38 of the same treaty provides a specific exemption for military transmissions. It allows members to retain their entire freedom with regard to military radio

stations. Since a significant portion of our routine military traffic utilizes civilian communications systems, this traffic is not protected by Article 38. The ITC makes it very clear that the military may not use civilian telecommunications satellites to project military power, but may use military satellite systems for such endeavors.[32]

International communications laws specify no direct prohibition against the conduct of wartime information operations by military forces. Throughout history, telecommunications treaties are suspended among belligerents during an international armed conflict, so wartime communications are fair game. Even in peacetime, violations of the ITC regulations may have minimal repercussions, especially for a country as significant in international communications as the U.S. Even if international sanctions appeared probable, the U.S. might decide that the benefit of conducting information operations against a particular adversary outweighs the possibility of international condemnation. Even when information operations activities do violate the ITU, mere violations are more than likely to be considered breaches of contractual obligations under the treaty than acts of war justifying a forceful response. In the final analysis, international communications laws do not appear to have much constraint against military operations. [33]

SPACE LAW

International law regulating activities in outer space may significantly apply to information operations because space segments are critical to international communications as well as to military information platforms providing military command, control, communications, and intelligence. Many information operations may involve orbital assets and thus fall under the jurisdiction of space law. The fundamental legal document governing space throughout the international community is the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the moon and other celestial bodies. The 1971 Agreement Relating to the International Telecommunications Satellite Organization (INTELSAT) and the 1976 Convention on the International Maritime Satellite Organization (INMARSAT) also affect telecommunications and the use of space. However, their relevance is limited to the principles of nondiscrimination among nations using the relevant satellites.[34]

Article IV of the Outer Space Treaty provides that outer space will be used exclusively for peaceful purposes. Since space exploration began in the early 1950's, two distinct schools of thought have arisen concerning the meaning of the peaceful purposes clause. One view is that the peaceful purposes clause applies only to non-military actions. The opposing view is that the term applies to non-aggressive actions. The U.S. has consistently held the position that

peaceful purposes are limited to non-aggressive actions. This view is based upon Article III, which provides that all space activities shall be conducted in accordance with the UN Charter. Since the UN Charter allows use of force in self-defense, the term peaceful purposes must also permit the use of defensive force and ban only aggressive, offensive acts, which are likewise banned by the UN Charter.[35]

Similarly, other parts of the Outer Space Treaty mention concepts like "common interest of all mankind," "benefits all people," "maintaining peace and security," and "use in accordance with international law," and provides a basis to support the "non-aggressive" interpretation. On this basis, outer space is to be used in a cooperative manner to benefit all people and in a manner which does not jeopardize international peace and security. Accordingly, the use of outer space for offensive information operations would be inconsistent with the UN Charter and therefore inconsistent with the Outer Space Treaty. As such, space laws and conventions complement the UN Charter regarding the use of force and threat of aggression. These laws, like the Charter, will not however prohibit the use of force in a self-defense posture.[36]

Many information operation activities could obstruct satellite communications. For example, one approach to impeding space systems is by targeting their ground stations. Another approach is to jam or spoof their communications links. Lastly, as we have seen during the war on terrorism in Afghanistan, the U.S. purchased all the commercial imagery that covers the Afghanistan area of operations. These separate and distinct ways to utilize information operation attacks are however subject to the general principles of international law, the U.N. Charter, and to a number of treaties obligations that applies specifically to space activities. [37]

NEUTRALITY AND NATIONAL SOVEREIGNTY

If a nation-state declares its neutrality during an armed conflict, it is then theoretically immune to premeditated attacks across its territorial borders. This immunity, however, is provisional. To qualify as neutral, these nations are prohibited against providing certain types of military support to any belligerent. If a neutral nation is unable or unwilling to deny the use of its territory by one of the belligerents in a manner that gives it a military advantage, the other belligerent has the right to attack its enemy in the neutral's territory. A neutral state's telecommunication infrastructure is immune from attack so long as it is made accessible to both sides in the conflict. But if a neutral nation allows its telecommunications infrastructure to be used only by the military forces of one belligerent, the other belligerent has a right to demand that the neutral nation stop doing so or provide the same access to his forces. If the neutral nation refuses, or for some reason is unable to prevent such use, the other belligerent may have

a limited right to self-defense to prevent such use by its enemy.[38] In a real world example, it is quite foreseeable that a belligerent might demand that a neutral nation not provide satellite imagery of the belligerent's forces to its enemy. If the neutral decides to continue providing the satellite imagery, then the neutral country could be seen as no longer neutral and be subject to attack from the other belligerent.[39]

The application of principles of neutrality will depend in part on the ability of states to identify discrete portions of a telecommunications network that legitimately can be called sovereign territory. Without such designations, it would be difficult to designate neutral areas except for tangible objects like satellites and computer hardware. Arguably, the neutrality of nation-states presents yet another possible concern regarding the international legality of information operations.

FOREIGN DOMESTIC LAWS

Other nations' legal structure may limit the U.S. information operations strategy. The complexity of foreign domestic laws applicable to technologically advanced information operations platforms will vary enormously from country to country. Despite such variations, foreign laws pose some implications for U.S. military information operations strategy for several fundamental reasons. First, a nation's criminal law can directly influence the assistance that the nation's government can provide in suppressing certain actions. Second, a nation's domestic laws may have a significant influence on U.S. information operations conducted in the nation's territory or communications routed through the nation's communications systems. For example, if a commander located in a host nation decides to conduct a specific information operations attack on another nation's assets, the commander needs to consider whether or not such activity is prohibited under local law. This implication is very important for two reasons: First, the commander who issues the order to conduct the information attack might be subject to prosecution in a host nation's criminal court. Lastly, the commander who knows that such an activity may violate host nation laws may decide not to conduct the operation. [40]

RECOMMENDATIONS

As discussed throughout this paper, the international legal community has not yet resolved inconsistencies regarding the categorization of information operations. Therefore, international law leaves room for the U.S. to conduct information operations. On the other hand, just as the U.S. can execute an information operations attack against an adversary, it can also be subjected to an information attack and limit our ability to take appropriate action in response

to such attacks. Our national leaders have several options to address the international legal implications of information operations.[41]

First, U.S. policymakers may accept the status quo and continue to work within the existing antiquated international body of law, allowing the U.S. to plan and execute information operations without considerable legal repercussions, thus providing maximum flexibility to our national security strategy. Since the U.S. leads the world in the development of its information operations technology, an international legal framework that permits information attacks could provide the U.S. a decisive advantage over its adversaries. Although the current international legal framework does not address particular information attacks as "armed attacks," "aggression," or "force," the U.S. could act with some assurance that its acts will not violate specific international law. Given the U.S. role in world politics and its superpower military stature, the U.S. portrays the positions of legislator and sheriff, possessing significant influence over the international community. [42]

Second, as a consequence of the rapid information-based technological revolution, U.S. policy-makers should seize the initiative and pursue international initiatives with the United Nations, the World Court, and other international organizations to develop a comprehensive body of international laws to resolve ambiguities over the employment of information operations. Given the U.S. position as the world's only superpower, our policy-makers could provide the leadership to establish an initial international legal framework, which could then encourage other countries to agree on certain standards, eventually integrating such agreements into traditional international law. Yet no law can change as swiftly as technology. In the interim, more immediate pressures for regulatory guidance may prompt nations to seek compromise through the treaty-making process. If only to increase protection of U.S. networks and telecommunication systems, then, specific nonexclusive legal or policy initiatives may be suitable.[43]

Additionally, the U.S. could pursue some type of arms control or specific ban on information operations attacks. Such an approach would provide clear legal norms to guide future actions and may become strategically advantageous if the U.S. were to determine that its vulnerabilities outweigh its technological advances. Unfortunately, such a ban on information operations attack may not be in the U.S. best interest. For example, limiting information attacks would not affect non-state actors, such as terrorist organizations who may be our greatest threat in future conflicts. Additionally, many information operations techniques have "dual-use" military and civilian uses, but their applications are predominantly utilized throughout the civilian sector.

Lastly, by initiating a ban on information operations attacks, the U.S. could be prematurely limiting a future weapon system that could minimize the lethality of future conflict.[44]

CONCLUSION

Information operations currently enable the U.S. to leverage its technological superiority to win our nation's wars in the most direct and feasible ways. Information operations enhance the means of our national leaders to accomplish the objectives set forth in the National Security Strategy. [45] Information operations have the potential to cause less casualties, decrease property damage, and put fewer American soldiers in harm's way. Ultimately, information operations may facilitate decisive victory at a reduced cost in bloodshed and financial resources.

Nations around the world have similar access to industrial technology that we enjoy in the U.S. today. These nations will employ information operations techniques, targeting facilities that could include electrical facilities, telecommunications networks, financial institutions, air-traffic control systems, rail traffic, waterways, and military communication networks. Certain types of information operations could violate particular international laws: the United Nations Charter, the Law of Armed Conflict, the International Telecommunications Law, Space Law, National Sovereignty Laws and Foreign Domestic Laws.

Unfortunately, there seems to be little likelihood that the international legal system will soon generate a comprehensive body of international law to guide the U.S. military's information operations strategy. Regrettably, the current outdated body of international law presents numerous challenges that could complicate our military's ability to execute information operations. In view of these legal ambiguities, the U.S. should plan and conduct information operations with considerable oversight and prudence, seeking a detailed legal review prior to executing specific actions. A practical approach to planning information operations within the current international legal framework would be to anticipate specific actions and make well-informed decisions about how these specific acts would be interpreted throughout the international legal community.[46]

In conclusion, this study identifies the widening gap between the effects of technology on warfare and the laws that preside over warfare, specifically as they relate to information operations. Transforming the Army is a significant challenge in itself. Transforming international laws of conflict so that they sufficiently address emerging military capabilities is an even more daunting challenge.

WORD COUNT = 6160

ENDNOTES

[1]David J. DiCenso, "IW Cyberlaw: The Legal Issues of Information Warefare," Airpower Journal; (Summer 1999): 13.

[2]Lawrence T. Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo, Information Warfare and International Law (Washington, D.C.: National Defense University Press, 1998): Introduction 1.

[3]Walter SharpSr., Cyber Space and the Use of Force. (Falls Church, VA.: Aegis Research Corp., 1999): XIV.

[4]Dennis Steele, "The Hooah Guide to Army Transformation," Army Magazine, February 2001, 1.

[5]Louis Caldera and Eric K. Shinseki, United States Army Transformation Campaign Plan (Washington D.C.: HQ Department of the Army, 2000): 1-4.

[6]U.S. Army War College. The Army Transformation: A Case Study (Carlisle Barracks, PA.: U.S. Army War College, 2000): 2.

[7]Steele, 5.

[8]U.S. Army War College. The Army Transformation: A Case Study, 3.

[9]Ibid, 5-7.

[10]Steele, 5.

[11]U.S. Army War College, Information Operation Primer (Carlisle Barracks, PA.: U.S. Army War College, 2001): 6&24.

[12]John L. Woodward, Information Assurance through Defense in Depth, Directive from the Director for Command, Control, Communications, and Computer Systems (J6), Joint Chiefs of Staff. Washington, D.C.: U.S. Department of Defense, 1997.

[13]Joint Chiefs of Staff, Joint Doctrine for Information Operations Joint Publication 3-13, (Washington, D.C.: U.S. Joint Chiefs of Staff, October 1998): I-6.

[14]Ibid, IV3.

[15]U.S. Department of the Army, Draft for revision Information Operations. Field Manual 3-13, (Washington, D.C.: 4 October 2000): Available from <http:/www-cgsc.army.mil /cdd/fm3-13/fm3-13.htm>; Internet; accessed 10 October 2001.

[16]U.S. Department of the Army, Force Structure Implications of the ACofS, G7, Information Operations White Paper. (Fort Leavenworth, U.S. Combined Arms Center, 9 July 2001): 2.

[17]Greenberg etal. Introduction 1-3.

[18]Ibid, 3.

[19]Ibid, 10-11.

[20]Ibid.

[21]Ibid.

[22]Walter Sharp, Cyber Space and the Use of Force. (Falls Church, VA.: Aegis Research Corp., 1999): 132-134 and 176-181.

[23]Ibid, 35.

[24]U.S.Department of Defense. An Assessment of International Legal Issues in Information Operations. (Washington, D.C.: U.S. Department of Defense, August 1999): 11-16.

[25]DiCenso, 3.

[26]Gregory J. O'Brian, The International Legal Limitations on Information Warfare, Masters Thesis. (Temple University Law School, 1998): 37-39.

[27]Ibid, 50-54.

[28]Ibid, 45-48.

[29]Ibid, 79.

[30]Ibid, 37.

[30]U.S. Department of Defense, 30.

[31]Ibid.

[32]Ibid.

[33]Greenberg etal, 1.

[34]Ibid, 2.

[35]O'Brian, 71-72.

[36]Ibid, 72-75.

[37]U.S. Department of Defense. An Assessment of International Legal Issues in Information Operations, 24.

[38]Greenberg, 3.

[39]U.S. Department of Defense. An Assessment of International Legal Issues in Information Operations, 9.

[40]Ibid, 39-41.

[41]Greenberg, 1.

[42] Ibid.

[43]Ibid, 1-4.

[44]Ibid, 3.

[45] Richard W. Aldrich, The International Legal Implications of Information Warfare, USAF Institute of National Security Studies Occasional Paper 9. (United States Air Force Academy, CO.: 1996), 3.

[46] U.S. Department of Defense. An Assessment of International Legal Issues in Information Operations, 48.

BIBLIOGRAPHY

Aldrich, Richard W. The International Legal Implications of Information Warfare. USAF Institute of National Security Studies Occasional Paper 9. United States Air Force Academy, CO.: April 1996.

Berra, Yogi. "Yogi-isms." Available from http://www.yogi-berra.com/yogiisms.html Internet Accessed 13 August 2001.

Caldera, Louis and Eric K. Shinseki. United States Army Transformation Campaign Plan, Washington, D.C.: HQ Department of the Army, 2000.

DiCenso, David J. "IW Cyberlaw: The Legal Issues of Information Warfare." Airpower Journal; (Summer 1999).

Greenberg, Lawrence T., Seymour E. Goodman and Kevin J. Soo Hoo. Information Warfare and International Law. Washington, D.C.: National Defense University Press, 1998.

Joint Chiefs of Staff. Information Warfare. Joint Publication, Washington, D.C.: U.S. Government Printing Office, December 1996.

Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Publication 3-13, Washington, D.C.: U.S. Government Printing Office, 9 October 1998.

Joint Chiefs of Staff. Joint Vision 2020. Washington, D.C.: U.S. Government Printing Office, June 2000.

Libicki, Martin C. What is Information Warfare? Washington, D.C.: National Defense University, October 1995.

O'Brian, Gregory J. The International Legal Limitations on Information Warfare, Masters Thesis. Temple University Law School, 1998.

Sharp, Walter Sr. Cyber Space and the Use of Force. Falls Church, VA.: Aegis Research Corp., 1999.

Shinseki, Eric K. "The Army Transformation: A Historic Opportunity." The Army Magazine, The Green Book, October 2000.

Shulman, Mark R. Legal Constraints on Information Warfare. Occasional Paper No. 7.Maxwell Air Force Base. March 1999.

Steele, Dennis. "The Hooah Guide to Army Transformation." Army Magazine, February 2001.

U.N. Charter, "Article 51, Chapter VII." Available from <http://www.un.org/aboutun/charter.>. Internet. Accessed 14 September 2001.

U.S. Army Public Affairs. "Army Announces Vision for the Future." 12 October 1999. Available from <http://www.dtic.mil/armylink/news/Oct1999/r19991015vision095.html>. Internet. Accessed 14 August 2001.

U.S. Army War College. Information Operation Primer. Carlisle Barracks, PA.: U.S. Army War College, January 2001.

U.S. Army War College. The Army Transformation: A Case Study. Carlisle Barracks, PA.: U.S. Army War College, October 2001.

U.S. Department of the Army. "Force Structure Implications of the ACofS, G7, Information Operations." White Paper. Fort Leavenworth, U.S. Combined Arms Center, 9 July 2001.

U.S. Department of the Army. The Army. Field Manual 1. Washington, D.C.: U.S. Department of the Army, 14 June 2001.

U.S. Department of the Army. Operations. Field Manual 3-0. Washington, D.C.: U.S. Department of the Army, 14 June 2001.

U.S. Department of the Army. "Draft" for revision Information Operations. Field Manual 3-13. Washington, D.C.: U.S. Department of the Army, 4 October 2000.

U.S. Department of Defense. An Assessment of International Legal Issues in Information Operations. Washington, D.C.: U.S. Department of Defense, August 1999.

U.S. Department of Defense. Information Operations. Department of Defense Directive S3600.1, Washington, D.C.: U.S. Department of Defense, 9 December 1996.

Woodward, John L., Information Assurance through Defense in Depth, Directive from the Director for Command, Control, Communications, and Computer Systems (J6), Joint Chiefs of Staff. Washington, D.C.: U.S. Department of Defense, 1997.